

Algebra: The Basics of It

Adair Antonio da Silva Neto

November 12, 2021

Contents

1	Introduction	1
2	Definitions	1
2.1	Ring	1
2.2	Domain	3
2.3	Field	3
3	Examples	3
3.1	Gaussian Integers	3
3.2	Direct product	3
3.3	Ring of integers modulo n	4
3.4	Ideal	4
3.5	Quotient ring modulo an ideal	5

1 Introduction

In this text, we'll assume just basic Set Theory, involving the concepts of relations, equivalence classes, Cartesian product and so on.

So... what is algebra about?

2 Definitions

2.1 Ring

Think about the set of integers \mathbb{Z} and the operations $+$ and \times on it. What properties do these operations satisfy?

We know that addition is associative and commutative and that it has a neutral element denoted by 0 and an inverse element.

With respect to multiplication, it is associative and commutative, it has a neutral element and the addition is distributive with respect to multiplication.

A ring is a generalization of these properties that we already know. In this section, we are going to study sets with two operations $+$ and \times that satisfy the properties elucidated above. These operations are not necessarily the addition and multiplication that we know for \mathbb{Z} .

Definition 2.1: Ring

A **commutative ring** $(A, +, \times)$ is a set A with at least two elements, an operation denoted by $+$ (called addition) and an operation denoted by \times (called multiplication) satisfying:

- A1) Addition is **associative**: $\forall x, y, z \in A, (x + y) + z = x + (y + z)$
- A2) Addition has a **neutral element**: $\exists 0 \in A$ such that $\forall x \in A, 0 + x = x$ and $x + 0 = x$.
- A3) Addition has an **inverse element**: $\forall x \in A, \exists z \in A$ such that $x + z = 0$ and $z + x = 0$.
- A4) Addition is **commutative**: $\forall x, y \in A, x + y = y + x$.
- M1) Multiplication is **associative**: $\forall x, y, z \in A, (x \times y) \times z = x \times (y \times z)$.
- M2) Multiplication has a **neutral element**: $\exists 1 \in A$ such that $\forall x \in A, 1 \times x = x$ and $x \times 1 = x$. 1 is also called **identity**.
- M3) Multiplication is **commutative**: $\forall x, y \in A, x \times y = y \times x$.
- D) Addition is **distributive** with respect to multiplication: $\forall x, y, z \in A, x \times (y + z) = x \times y + x \times z$.

We may denote $a \times b$ by $a \cdot b$ or simply ab and context will elucidate.

If, for a given ring, all these properties are satisfied except for the commutative of multiplication, then we'll call it a non-commutative ring.

Some important remarks:

- The neutral element is unique, both for addition and multiplication.
- The inverse element, with respect to addition, is unique.
- The neutral element of addition has the following property: $0 \cdot x = 0, \forall x \in A$.

We also define a **subring** of a ring as the subset which is closed under the operations of addition, subtraction, and multiplication and also contains the element 1 .

Before heading to some examples, let give two important definitions.

2.2 Domain

If the product of any two non-zero elements of a given ring D is different than zero, then this ring is called a **domain** or an **integral domain**.

$$M_4) \forall x, y \in D \setminus \{0\}, x \times y \neq 0$$

Hence, if D is an integral domain, $a, b, c \in D$ and $ab = ac$, then $a \neq 0$ implies $b = c$. This is called **cancellation law**.

An immediate example of a domain is $(\mathbb{Z}, +, \times)$.

2.3 Field

If every non-zero element of a given ring has a multiplicative inverse, then this ring is called a **field**. Symbolically,

$$M_4') \forall x \in K \setminus \{0\}, \exists y \in K : x \times y = 1$$

This inverse is also unique and the inverse of x is denoted by x^{-1} .

Please take notice that this property is stronger than the property that defines a domain. That means that if K is a field, then K is also a domain. Although not all domains are fields, if the domain has a finite number of elements, then it is a field.

E.g. $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$ are fields.

3 Examples

3.1 Gaussian Integers

Let $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$. Then $(\mathbb{Z}[i], +, \times)$ is a domain called **Gaussian integers**. This idea can be generalized by defining a subring generated by n as $\mathbb{Z}[n]$.

3.2 Direct product

Given two rings $(A_1, +_1, \cdot_1)$ and $(A_2, +_2, \cdot_2)$, it's possible to construct a new ring defining:

- The set $A_1 \times A_2 := \{(a_1, a_2) \mid a_1 \in A_1, a_2 \in A_2\}$
- Addition: $(a_1, a_2) + (a'_1, a'_2) := (a_1 +_1 a'_1, a_2 +_2 a'_2)$
- Multiplication: $(a_1, a_2) \times (a'_1, a'_2) := (a_1 \cdot_1 a'_1, a_2 \cdot_2 a'_2)$.

Then $(A_1 \times A_2, +, \cdot)$ is a ring called **direct product** of A_1 and A_2 .

3.3 Ring of integers modulo n

Let $n \in \mathbb{Z}_+$ and define the relation \equiv_n as: given $a, b \in \mathbb{Z}$,

$$a \equiv_n b \iff a - b \text{ is a multiple of } n$$

And we say that a is congruent to b modulo n . Notice that \equiv_n is an equivalence class.

The equivalence class of a is denoted by $\bar{a} = \{b \in \mathbb{Z} \mid b \equiv_n a\} = \{a + kn, k \in \mathbb{Z}\}$.

We also write $\mathbb{Z}/n\mathbb{Z}$ to denote the set of equivalence classes modulo n , i.e. $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$. And we define the following compositions over it:

$$\begin{aligned} \oplus_n : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} &\rightarrow \mathbb{Z}/n\mathbb{Z} \\ (\bar{x}, \bar{y}) &\mapsto \overline{x+y} \\ \odot_n : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} &\rightarrow \mathbb{Z}/n\mathbb{Z} \\ (\bar{x}, \bar{y}) &\mapsto \overline{xy} \end{aligned}$$

Then $(\mathbb{Z}/n\mathbb{Z}, \oplus_n, \odot_n)$ is a ring, where the neutral element for \oplus_n is the class $\bar{0}$, the neutral element for \odot_n is $\bar{1}$, and the inverse of \bar{x} with respect to \oplus_n is the class $\overline{-x}$.

3.4 Ideal

Before going to next example, a simple definition is necessary.

Definition 3.1: Ideal

If $I \subseteq A$, $I \neq \emptyset$, then I is called an **ideal** of A if

- $x + y \in I, \forall x, y \in I$.
- $ax \in I, \forall x \in I, \forall a \in A$.

For example, $n\mathbb{Z} := \{zn \mid z \in \mathbb{Z}\}$ is an ideal of the ring of integers (where n is a non-negative integer).

This concept allows us to make constructions analogous to the ring of integers modulo n . In general, an ideal is not a ring because it usually lacks a neutral element.

3.5 Quotient ring modulo an ideal

Given a ring A and I an ideal of A , define the following congruence relation: for $a, b \in A$,

$$a \equiv b \pmod{I} \iff a - b \in I$$

Which is also an equivalence relation.

If $a \in A$, then its class of equivalence modulo I is given by $\bar{a} := \{b \in A \mid b \equiv a \pmod{I}\} = \{a + c \mid c \in I\}$. We denote A/I the set of equivalence classes modulo I , and we define the following operations over it: for $\bar{x}, \bar{y} \in A/I$,

$$\bar{x} \oplus_I \bar{y} := \overline{x + y} \text{ and } \bar{x} \odot_I \bar{y} := \overline{x \cdot y}$$

These operations are well defined and $(A/I, \oplus_I, \odot_I)$ is a ring called **quotient ring modulo an ideal**.

References

- [Art91] Michael Artin. *Algebra*. Prentice-Hall, 1991.
- [GLO6] Arnaldo Garcia and Yves Lequain. *Elementos de álgebra*. Instituto de Matemática Pura e Aplicada, 2006.
- [Lee18] Gregory T Lee. *Abstract algebra: An introductory course*. Springer, 2018.